Prof. Dr. Heinrich Amadeus Wolff, Universität Bayreuth

Die gegenwärtige Situation des Datenschutzes in Deutschland[1]

I. Einleitung

1. Was ist Datenschutz?

Datenschutz will die Verarbeitung von personenbezogenen Daten regeln. Personenbezogene Daten sind Einzelangaben über eine bestimmte oder bestimmbare Person.[2] Verarbeitung ist jeder Umgang mit diesen Daten,[3] insbesondere Erhebung, Speicherung, Löschung, Änderung und Nutzung.[4] Diese ist nicht frei möglich. Die Art der Daten ist unerheblich. Auch belanglose Daten werden geschützt.[5] Diese Perspektive ist vom Ansatz her befremdlich, weil man aufgrund allgemeiner Kommunikationsregeln denkt, dass jemand einen Anspruch benötigt, wenn er von einer anderen Person möchte, dass diese etwas vergessen soll. Diese Regeln werden vom Datenschutz umgedreht. Vereinfacht gesprochen muss derjenige, der sich etwas merken will, dafür einen Rechtsgrund anführen. Es ist sehr zweifelhaft, ob dieser Ansatz gedanklich richtig ist, er ist aber dennoch Grundlage des Datenschutzrechts. Der Datenschutz bildet einen erheblich vorgelagerten Persönlichkeitsschutz.[6] Er greift schon dann ein, wenn die Persönlichkeit selbst noch nicht gefährdet ist. Anknüpfungspunkt ist allein der Charakter einer Information als personenbezogenes Datum. Wer Daten anderer Personen verarbeiten will, bedarf dafür grundsätzlich einen Rechtsgrund.[7]

II. Die tragenden Prinzipien des Datenschutzes

Die tragenden Prinzipien des Datenschutzes sind:

1. Das Verbotsprinzip

Das Datenschutzrecht normiert folgendes Verbotsprinzip: Das Verarbeiten personenbezogener Daten ist grundsätzlich verboten, es sei denn, der Verarbeiter kann sich auf einen Erlaubnisgrund berufen.[8] Dieses Prinzip ist in Deutschland unabhängig vom Datenschutz üblich, sofern es um einen Eingriff des Staates in Freiheit und Eigentum bzw. um Grundrechtseingriffe geht.[9] Beim Datenschutz ist dieses Prinzip aber deutlich ausgeweitet und meint, dass zunächst jede staatliche Verarbeitung einer Rechtfertigung bedarf, auch wenn sie banal ist und man eigentlich über den Eingriffscharakter streiten könnte. Darüber hinaus sind auch Verarbeitungen durch Private, von denen keine Grundrechtsein-

---

1 Schriftliche Fassung eines Vortrags, den der Autor im März 2018 an der Chinese Culture University (PCCU) in Taipeh (Taiwan) halten wird. Der Aufsatz soll in einer chinesischen Übersetzung in Taiwan erscheinen.

2 § 3 Abs. 1 Bundesdatenschutzgesetz-alt (BDSG-alt) – s. http://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html.BDSG-alt; in gleicher Weise Art. 4 Abs. 1 Datenschutz-Grundverordnung (Fn. 46).

3 Art. 4 Abs. 2 Datenschutz-Grundverordnung (Fn. 46).

4 § 3 Abs. 2 BDSG-alt (Fn. 44).

5 BVerfGE 65, 1, 45 – s. http://www.servat.unibe.ch/dfr/bv065001.html.

6 BVerfGE 65, 1, 41 – s. http://www.servat.unibe.ch/dfr/bv065001.html.

7 § 4 Abs. 1 BDSG-alt (Fn. 44); Art. 7 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:31995L0046.

8 § 4 Abs. 1 BDSG-alt (Fn. 44); Art. 7 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:31995L0046.

9 BVerfGE 65, 1 (45) - s. http://www.servat.unibe.ch/dfr/bv065001.html.

griffe ausgehen können, rechtfertigungsbedürftig.[10] Das Verbotsprinzip führt dazu, dass der Staat im Eingriffsbereich immer zwei Rechtsgrundlagen benötigt: Eine, der ihm den Eingriff in die Grundrechte des Bürgers gestattet und eine, die es ihm erlaubt, die dazugehörigen Daten zu verarbeiten.

Das Verbotsprinzip verliert erheblich an Brisanz, weil es allgemeine Rechtsgrundlagen gibt, nach denen die Verwaltung all die Daten verarbeiten darf, die sie benötigt, um ihre Aufgaben zu erledigen. [11] Weitere wichtige Rechtsgrundlagen sind:

- die Einwilligung des Betroffenen, die freiwillig, informiert und klar erklärt werden muss und grundsätzlich widerruflich ist; [12]
- die Berechtigung Daten zu verarbeiten, um einen Vertrag zu erfüllen oder um eine gesetzliche Pflicht zu erfüllen; [13]
- die (im privaten Bereich wichtige) Erlaubnis, Daten zu verarbeiten, wenn das Interesse des Facharbeiters das Interesse der betroffenen Person überwiegt. [14]

Diese allgemeinen Rechtsgrundlagen genügen nur für Verarbeitungen, die eine unterstützende Funktion besitzen. Verarbeitungen, bei denen der primäre Zweck in der Verarbeitung, insbesondere in der Informationsgewinnung besteht und von denen eine erhebliche Eingriffsintensität oder ein anderes Gewicht ausgeht, weil es um Informationserhebungen im sensiblen Grundrechtsbereich geht, bedürfen eine ganz konkrete und bestimmte Rechtsgrundlage, die gerade die Erhebung dieser Art rechtfertigt.[15] Dies ist nicht im Datenschutz selbst niedergelegt, sondern folgt aus den Grundrechten. Sensible Grundrechtsbereiche sind dabei vor allem: das Grundrecht auf Wohnung; das Brief-, Post- und Fernmeldegeheimnis; der Schutz vor einem Eingriff in die Datenbanken persönlicher digitaler Geräte wie Laptop und Computer; der Schutz vor längerfristiger Observation. Nach dem BVerfG sind heimliche Überwachungsmaßnahmen, die tief in die Privatsphäre eingreifen, mit der Verfassung nur vereinbar, wenn sie dem Schutz oder der Bewehrung von hinreichend gewichtigen Rechtsgütern dienen, für deren Gefährdung oder Verletzung im Einzelfall belastbare tatsächliche Anhaltspunkte bestehen. Sie setzen grundsätzlich voraus, dass der Adressat der Maßnahme in die mögliche Rechtsgutsverletzung aus Sicht eines verständigen Dritten den objektiven Umständen nach beteiligt oder verantwortlich ist.[16] Die Informationserhebung muss auf den Schutz oder die Bewehrung hinreichend gewichtiger Rechtsgüter begrenzt sein,[17] deren Bedrohung absehbar ist. Erforderlich ist eine vorherige Kontrolle durch eine unabhängige Stelle.[18] Der Kernbereich privater Lebensgestaltung muss wirkungsvoll geschützt bleiben.[19] Es darf insgesamt nicht zu einer Vollüberwachung kommen.[20] Berufs- und anderen Personengruppen, deren Tätigkeit von Verfassungs wegen eine besondere Vertraulichkeit voraus-

---

10 *Bäcker*, in: Wolff/Brink (Hg.), BeckOK-Datenschutzrecht, § 4 BDSG, (22. Edition- Stand: 01.02.2017), Rn. 3 – s. https://beck-online.beck.de/?vpath=bibdata\komm\BeckOKDatenS_22\BDSG\cont\BECKOKDATENS.BDSG.P4.glA.glI.htm (kostenpflichtiger Zugang).

11 § 13, § 14 BDSG-alt (Fn. 44); Art. 6 Abs. 1 UAbs. 1 lit. e) Datenschutz-Grundverordnung (Fn. 46); § 3 BDSG-neu (Fn. 48).

12 §§ 4, 4a BDSG-alt (Fn. 44); Art. 6 Abs. 1 UAbs. 1 lit. a), Art. 7, Art. 8 Datenschutz-Grundverordnung (Fn. 46).

13 § 28 Abs. 1 Nr. 1 BDSG-alt (Fn. 44); Art. 6 Abs. 1 UAbs. 1 lit. b) Datenschutz-Grundverordnung (Fn. 45).

14 § 28 Abs. 1 Nr. 2 BDSG-alt (Fn. 44); Art. 6 Abs. 1 UAbs. 1 lit. f) Datenschutz-Grundverordnung (Fn. 45).

15 BVerfG, Ut. v. 20.04.2016, 1 BvR 966/09 u.a.), Rn. 103; s. http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html

16 BVerfG, Ut. v. 20.04.2016, 1 BvR 966/09 u.a. (Fn. 15), Rn. 104

17 BVerfG, Ut. v. 20.04.2016, 1 BvR 966/09 u.a. (Fn. 15), Rn 106

18 BVerfG, Ut. v. 20.04.2016, 1 BvR 966/09 u.a. (Fn. 15), Rn. 117.

19 BVerfG, Ut. v. 20.04.2016, 1 BvR 966/09 u.a. (Fn. 15), Rn. 119 ff.

20 BVerfG, Ut. v. 20.04.2016, 1 BvR 966/09 u.a. (Fn. 15), Rn. 131.

setzt, sind hier ausreichend zu schützen.[21] Der Betroffene ist schließlich über die Informationserhebung zu informieren, wenn der Zweck der Maßnahme dies zulässt.[22]

2. Prinzip der Schutzbereichsräume (eigener Begriff)

Der Anknüpfungspunkt des Datenschutzrechtes sind Daten. Daten sind omnipräsent wie die Luft oder das Licht. Dennoch ist das Datenschutzrecht selbst nicht omnipräsent. Vielmehr existieren Datenschutzbereiche.[23] Ein Teil dieser Datenschutzräume ergibt sich aus der Natur der Sache, teilweise werden sie vom Gesetzgeber bestimmt. Folgende Räume lassen sich unterscheiden:

- Keine Datenschutzregelung gibt es für eine Verarbeitung, die allein im menschlichen Gehirn funktioniert.
- Vom einfachen Recht geschützt sind nur die Daten von natürlichen Personen. Die Daten von juristischen Personen fallen nicht unter das einfache Datenschutzrecht.[24]
- Frei von spezifischem Datenschutz ist die Datenverarbeitung durch Private allein zu privaten Zwecken.[25]
- Sonderregelungen gibt es weiter für die Bereiche Presse, Journalismus und Kirchen. [26]
- Für die Rechtsprechung gilt zwar das Datenschutzrecht, kontrolliert wird ihre Datenverarbeitung aber nur, sofern es um Verwaltungstätigkeit der Gerichte geht;[27]
- Aufgrund der Kompetenzverteilung zwischen Europa und Deutschland gibt es drei Regelungsräume:[28] den Bereich der Verarbeitung zur Straftatenverfolgung und Verhütung, den allgemeinen europäischen Bereich und den Bereich, der nur von den Mitgliedsstaaten geregelt wird und der schwer zu bestimmen ist. Dazu gehören zumindest: Datenverarbeitung zu militärischen Zwecken, Datenverarbeitung der Nachrichtendienste/Geheimdienste, Datenverarbeitung für Begnadigungen und die Datenverarbeitung für Orden und Ehrenbürgerverleihungen.[29]

3. Zweckbindung

Der Zweckbindungsgrundsatz ist das Datenschutzprinzip, das den Datenschutz von anderen Rechtsgebieten deutlich trennt. Er gibt dem Datenschutz sein eigenes Gepräge. Die Heraushebung und Herausarbeitung dieses Prinzips war eine der besonderen Leistungen des Volkszählungsurteils des Bundesverfassungsgerichts.[30] Der Zweckbindungsgrundsatz besagt: Personenbezogene Daten dürfen nur für den Zweck verwendet werden, für den sie rechtmäßig erhoben wurden und der vor der Erhebung festgelegt wurde.[31] Das Motiv des Zweckbindungsgrundsatzes besteht in einer Eingrenzung der Verwendung personenbezogener Daten. Der Zweckbindungsgrundsatz knüpft an eine Zweckbestim-

---

21 BVerfG, Ut. v. 20.04.2016, 1 BvR 966/09 u.a. (Fn. 15), Rn. 131 ff.

22 BVerfG, Ut. v. 20.04.2016, 1 BvR 966/09 u.a. (Fn. 15), Rn. 134 ff.

23 *Wolff*, in: Wolff/Brink (Fn. 10)(Hg.), Prinzipien des Datenschutzrechts, Rn. 2; *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 451 ff. – s. https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2FSchantzWolffHdbNeuDSR_1%2Fcont%2FSchantzWolffHdbNeuDSR.Inhaltsverzeichnis.htm&anchor=Y-400-W-SCHANTZWOLFFHDBNEUDSR (kostenpflichtiger Zugang).

24 S. Fn. 2.

25 Art. 2 Abs. 2 lit. c) Datenschutz-Grundverordnung (Fn. 45).

26 Art. 85 und Art. 91 Datenschutz-Grundverordnung (Fn. 46).

27 Art. 55 Abs. 3, Art. 37 Abs.1 lit. a) Datenschutz-Grundverordnung (Fn. 46).

28 S. §§ 1-44 BDSG-neu (Fn. 48) i.V.m. DSGVO/ §§ 1-21 i.V.m. §§ 45-84 und §§ 1-21 i.V.m. § 85 BDSG-neu (Fn. 48).

29 *Wolff*, in: Schantz/Wolff, Datenschutzrecht, 2017 (Fn. 23), Rn.254.

30 BVerfGE 65, 1 (46) s. http://www.servat.unibe.ch/dfr/bv065001.html

31 Art. 5 Abs. 1 lit. b) Datenschutz-Grundverordnung (Fn. 46).

mung an und bindet die Daten an diese. Will man die Zweckbindung und die Daten voneinander lösen, benötigt man dafür wiederum eine neue Rechtsgrundlage. [32]

4. Grundsatz der Erforderlichkeit

Der Grundsatz der Erforderlichkeit lautet: Eine Datenverarbeitung personenbezogener Daten ist nur soweit zulässig, soweit diese zur Erreichung des Zwecks notwendig ist. [33] Der Grundsatz der Erforderlichkeit setzt eine rechtmäßige Datenverarbeitung und eine rechtmäßige Zweckbestimmung der Datenverarbeitung voraus und grenzt diese noch einmal ein. Er ist entwickelt worden für Datenverarbeitungen, die sich auf Rechtsnormen stützen, wird heute aber auf die Einwilligung erstreckt. Ein Rechtsgrund für eine Verarbeitung erlaubt nicht, dass alle Daten herangezogen werden, die nützlich sein können, sondern nur die Daten, die konkret geboten sind, zur Erreichung eines konkret festgelegten Zwecks.[34] Der Grundsatz der Erforderlichkeit setzt die Kenntnis des Zwecks der Datenverarbeitung voraus. Der Grundsatz der Erforderlichkeit verlangt nach zutreffender Auffassung aber nicht nur, dass eine Datenverarbeitung unterbleibt, die für die Zwecke überhaupt keinen Vorteil bringt. Er verlangt auch, dass keine alternative Form der Datenverarbeitung besteht, die die Zwecke in vergleichbarer Weise erreichen kann und zugleich als datenschutzschonender zu qualifizieren ist (Gebot der datenschutzschonenderen oder datenschutzintensiveren Alternative).[35] Komplizierte Formen der Arbeitsabläufe, die unsinnige Mengen von personenbezogenen Daten anhäufen, genügen dem Erforderlichkeitsgrundsatz auch dann nicht, wenn sie die Zweckerreichung objektiv gesehen noch unterstützen.[36] Nicht gemeint ist, dass der Gedanke der Optimierung von Verarbeitungsprozessen allein darin besteht, welche Variante die geringste Datenverarbeitung benötigt.

5. Grundsatz der Direkterhebung

Der Grundsatz der Direkterhebung lautet: Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben. Eine Erhebung in anderer Weise bedarf einer sachlichen Rechtfertigung. Der Grundsatz ist nicht sehr streng umgesetzt.[37] Er ist aber der sachliche Grund dafür, dass man die betroffenen Person grundsätzlich informieren muss, wenn man Daten über sie bei Dritten erhebt.

6. Verbot der Vorratsdatenspeicherung

Aus dem Grundsatz der Zweckbestimmung und aus dem Grundsatz der Erforderlichkeit folgt das Verbot der Vorratsdatenspeicherung. Das Verbot der Vorratsdatenspeicherung besagt: Die Erhebung von Daten, ohne dass die Daten für einen konkreten Zweck benötigt werden, ist grundsätzlich unzulässig.[38] Eine Vorratsdatenspeicherung liegt dann vor, wenn Daten erhoben werden, ohne dass man mit Recht behaupten kann, diese Daten für einen bestimmten Verwaltungs- oder Geschäftszweck (der über das Datensammeln hinausgeht) mit hinreichender Sicherheit zu benötigen.

Eine selbständige Ausprägung besitzt dabei das Gebot der anlassbezogenen Datenerhebung. Dieses Gebot ist bisher nicht ausdrücklich formuliert und bislang nur der Sache nach anerkannt. In den Fallkonstellationen, in denen unklar ist, wie viele Daten die verarbeitende Stelle für die Zweckerreichung benötigt, muss die verarbeitende Stelle nach diesem Prinzip erst einmal so viele Daten erheben wie sie benötigt, um die erste anstehende Aufgabe zu bewältigen, und darf erst bei Anlass weitere Daten für die Erreichung der zweiten Stufe erheben.

---

32 Art. 6 Abs. 4 Datenschutz-Grundverordnung (Fn. 46).

33 Art. 6 Abs. 1 Datenschutz-Grundverordnung (Fn. 46); *Wolff*, in: Schantz/Wolff, Datenschutzrecht, 2017 (Fn. 23), Rn.254.

34 E EuGH Urt. v. 16. 12. 2008, Rs. C-l524/06 – Huber: Ausländerzentralregister, Rn. 47.

35 *Wolff*, in: Schantz/Wolff, Datenschutzrecht, 2017 (Fn. 23), Rn. 434 ff.

36 *Wolff*, in: Schantz/Wolff, Datenschutzrecht, 2017 (Fn. 23), Rn. 429 ff.

37 S. § 4a BDSG-alt; s.a *Wolff*, in: Schantz/Wolff, Datenschutzrecht, 2017 (Fn. 23), Rn. 456.

38 BVerfGE 125, 260 (317), s. http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintVersion&Name=bv125260.

7. Weitere Untergebote:

Es gibt noch eine Reihe weniger zentraler Datenschutzprinzipien. Genannt werden sollen noch:

- Gebot der Datensparsamkeit: Nach dem Grundsatz der Datenvermeidung und Datensparsamkeit sind prinzipiell so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.[39] Es sind grundsätzlich solche Datenverarbeitungsprozesse zu entwickeln, die mit möglichst wenigen Daten auskommen. Dabei ist vor allem auf Datenverarbeitungsprozesse umzustellen, bei denen die Verarbeitung anonymisierter oder pseudonymisierter Daten genügt.
- Prinzip der Transparenz: Der Grundsatz der Transparenz bedeutet: Die Datenverarbeitung insgesamt muss für den Betroffenen möglichst nachvollziehbar sein.[40]
- Gebot der Richtigkeit: Das Gebot der Richtigkeit besagt: Die verarbeitende Stelle hat Sorge dafür zu tragen, dass personenbezogene Daten sachlich richtig sind.[41]
- Gebot der Dauerrechtfertigung: Die Rechtfertigung einer Datenverarbeitung muss in jedem Augenblick ihrer Verarbeitung vorliegen. Fällt die Rechtfertigung weg, muss die Verarbeitung eingestellt werden, sofern dies technisch möglich ist.

III. Spannungen zwischen europäischem und deutschem Datenschutzrecht

1. Veränderungen durch Internationalisierung

Der Datenschutz besitzt in Deutschland eine lange Tradition und eine erhebliche Bedeutung. Deutschland ist der Auffassung, das erste Datenschutzgesetz der Welt im Jahr 1970 erlassen zu haben.[42] Trotz seines Alters ist der Datenschutz zurzeit erheblich in Bewegung. Der Grund liegt darin, dass Deutschland den Datenschutz nicht mehr alleine regeln kann. Deutschland ist, wie Sie vermutlich wissen, Teil der Europäischen Union.

Die europäische Union kann Rechtsakte mit unmittelbarer Wirkung gegenüber dem Bürger in Europa erlassen und kann auch Regeln erlassen, die sich an die Mitgliedstaaten richten und von diesen umgesetzt werden müssen.[43] Europa hat im Jahr 2016 seinen Datenschutz erheblich verändert. Insbesondere hat es den Datenschutz jetzt mit unmittelbarer Wirkung für die Unionsbürger normiert und verlangt nicht mehr, wie vorausgehend, eine Umsetzung durch nationales Recht. Bisher hat auf Bundesebene das Bundesdatenschutzgesetz gegolten, das im Mai 2018 außer Kraft treten wird (hier abgekürzt BDSG-alt).[44] Das BDSG hat eine alte europäische Richtlinie umgesetzt, die auch im Mai 2018 außer Kraft treten wird (die sogenannte Datenschutzrichtlinie).[45] Ab Mai 2018 wird das neue europäische Recht anwendbar sein, das vor allem aus unmittelbar anwendbaren Regeln für die Verarbeitung von Privaten und weiten Teilen der Verwaltung besteht - sogenannte Datenschutzgrundverordnung.[46] Für die Strafverfolgung und Straftatverhütung im weiteren Sinne gibt es Sonderregelungen,

---

39 Art. 5 Abs. 1 lit. c Datenschutz-Grundverordnung (Fn. 46); § 3a BDSG-alt.

40 Art. 12 Datenschutz-Grundverordnung (Fn. 46).

41 Art. 5 Abs. 1 lit.d) Datenschutz-Grundverordnung (Fn. 46); Wolff, in: Schantz/Wolff, Datenschutzrecht, 2017 (Fn. 23), Rn. 441.

42 Wolff, in: Schantz/Wolff, Datenschutzrecht, 2017 (Fn. 23), Rn. 2.

43 Art.288 AEUV.

44 Bundesdatenschutzgesetz (BDSG) – s. http://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html.

45 Datenschutzrichtlinie (Richtlinie des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [DSRL])- http://eur-lex.europa.eu/legal-content/DE-EN/TXT/?uri=CELEX:31995L0046&from=DE

46 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und

die in einer europäischen Richtlinien niedergelegt sind.[47] Diese Änderungen auf europäischer Ebene hat eine Änderung der deutschen Gesetze erforderlich gemacht. Das neue Bundesdatenschutzgesetz wurde erlassen mit dem Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017.[48] Auch wenn die grundlegenden Prinzipien des Datenschutzes in Deutschland und Europa weitgehend gleich sind, bestehen in der Gewichtung gewisser Unterschiede, die dazu führen, dass das deutsche Datenschutzrecht sich der Sache nach verändern muss. Diese Änderung kann dabei entweder in Form einer Ergänzung oder einer Änderung bestehen.

- Europa trennt erheblich zwischen einem freien Datenfluss in Europa und einer Übermittlung von personenbezogenen Daten außerhalb von Europa.[49] Zu einem Verarbeiter außerhalb von Europa dürfen Daten nur übermittelt werden, wenn generell oder zumindest im Einzelfall sichergestellt ist, dass beim Empfänger ein vergleichbares Datenschutzniveau wie in Europa besteht, oder einer der enumerativ aufgeführten Ausnahmefälle vorliegt.[50] Das deutsche Recht war zunächst auf Deutschland bezogen und musste insoweit ergänzt werden.
- Das europäische Recht achtet stärker auf die Datenqualität. Für das europäische Recht sind entscheidende Fragen; Wo kommen die Daten her? Wie hoch ist die Gewähr für die Richtigkeit? Welche Art von Daten sind es? Das deutsche Recht wurde entsprechend ergänzt.
- Das europäische Recht normiert starke Betroffenenrechte und vor allem starke Informationsrechte.[51] Das deutsche Recht kannte diese Rechte nur in schwächerer Form. Es hat nun teilweise seine Position verändert, teilweise aber auch von Ausnahmenmöglichkeiten Gebrauch gemacht.[52]
- Das europäische Recht sah eine Pflicht des Verarbeiters vor, erhebliche Datenschutzpannen an die Aufsichtsbehörde selbst zu melden. Diese Selbstbelastung bei dem deutschen Recht fremd und wurde nun eingeführt.[53] Das deutsche Recht hat dabei normiert, dass diese Meldung in einem Strafverfahren nicht zu Lasten des Betroffenen verwendet werden darf;[54] ob dies mit Europarecht vereinbar ist, ist fraglich.
- Das europäische Recht kennt die Möglichkeit der Selbstregulierung der Wirtschaft, in Form von Zertifikaten, Verhaltensregeln und unverbindlichen internen Regelungen.[55] Das deutsche Recht hat dies übernommen. Die Praxis nimmt diese Instrumente nicht an. Es handelt sich weitgehend um totes Recht.

---

zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung; s. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1517513016318&uri=CELEX:32016R0679.

47 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

48 BGBl I 2097 - s. https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id='bgbl117s2097.pdf']#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1517397588857; s. dazu die Gesetzesmotive BT-Drs. 18/11325 – s. http://dipbt.bundestag.de/doc/btd/18/113/1811325.pdf.

49 Art. 44 Datenschutz-Grundverordnung (Fn. 46); s. dazu *Schantz*, in: Schantz/Wolff (Fn. 33), Datenschutzrecht, 2017, Rn. 757 ff.

50 Art. 49 Datenschutz-Grundverordnung (Fn. 46).

51 Art. 12 Datenschutz-Grundverordnung (Fn. 46).

52 §§ 32-37 BDSG-neu (Fn. 48).

53 § 42a BDSG-alt.

54 § 42Abs. 4 BDSG; s.a. Wolff, in: Schantz/Wolff (Fn. 33), Datenschutzrecht, 2017, Rn. 915.

55 Art. 40-Art. 43 Datenschutz-Grundverordnung (Fn. 46).

- Das europäische Recht kennt eine starke Sonderstellung der Aufsichtsbehörden.[56] Die Aufsichtsbehörden dürfen monopolartig die Verletzung des Datenschutzrechts prüfen und sind völlig unabhängig von einer staatlichen Aufsicht. Das deutsche Recht kennt ein Gebot hinreichend demokratischer Legitimation jeder staatlichen Stelle.[57] Nur in Ausnahmefällen dürfen die Behörden völlig unabhängig sein. Nach deutscher Sichtweise dürfen die Aufsichtsbehörden bei der Kontrolle von Verarbeitern der freien Wirtschaft nicht völlig unabhängig sein. Deutschland weigerte sich daher zunächst das Europarecht umzusetzen und wurde vom EuGH verurteilt.[58] Nun wurde das deutsche Recht angepasst.
- Das Europarecht sieht scharfe Sanktionen bei Verstößen vor und lässt dafür in der Regel die Kausalität oder die Verursachung genügen.[59] Deutschland verlangt über die Kausalität hinaus noch ein Verschulden. Verschulden mein Vorsatz oder Fahrlässigkeit. Deutschland versucht nun das Erfordernis des Verschuldens bei den Sanktionen zusätzlich einzubauen.[60] Ob dies europarechtlich zulässig ist, ist umstritten. Ich selbst denke, es ist zulässig.[61]

IV. Schwierigkeiten des gegenwärtigen Datenschutzes

Europa hat, wie am Anfang erwähnt, 2016 sein Recht geändert und die Mitgliedstaaten somit auch. Sie sind verpflichtet bis Mai 2018, d.h. bis in vier Wochen, ihr Recht zu ändern. Deutschland hat die entsprechenden Rechtsakte schon erlassen, die in vier Wochen in Kraft treten werden. Das europäische Recht verlangt, soweit es unmittelbare Regelungen vorgibt, dass diese beachtet werden. Die Mitgliedstaaten dürfen das europäische Recht in der Regel nicht einmal wiederholen, geschweige denn es konkretisieren.[62] Beim Datenschutz ist aber oft ganz unklar, wie weit das unmittelbar anwendbare Recht reicht. Das europäische Recht ist ungewöhnlich unbestimmt, aus folgenden Gründen:

- Es gibt wie oben dargelegt zwei Reformakte von Europa. Einen Akt speziell für die Verarbeitung durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung und Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Daneben gibt es einen weiteren Akt für die sonstige Datenverarbeitung, der deutlich wichtiger, inhaltlich aber nicht ganz identisch ist. Die Abgrenzung der beiden Rechtsakte ist ganz unklar, insbesondere der Bereich der Abwehr von Gefahren der öffentlichen Sicherheit ist umstritten.[63]
- Viele Normen des unmittelbar geltenden Rechts sind alt und kommen aus einer Zeit, in der sich das europäischen Datenschutzrecht noch an die Mitgliedstaaten und noch nicht unmittelbar an die Bürger gerichtet hat.[64] Diese Regeln, die sich an die Mitgliedstaaten richten, sind aber anders formuliert als die, die sich an die Bürger richten, da sie auf eine Umsetzung ausgerichtet sind. Werden diese Regeln nun übernommen, sind sie notwendig unbestimmt.

---

56 Ar.t 51-59 Datenschutz-Grundverordnung (Fn. 46).

57 BVerfGE 83, 60 (73) s. http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintVersion&Name=bv093037; BVerfGE 93, 37 (67 ff.); BVerfGE 107, 59 (92 ff.); BVerfGE 111, 191 (216 ff.) s. http://www.servat.unibe.ch/dfr/bv111191.html.

58 EuGH Urt. v. 14,10.2008, Rs. C-518/07 (Kommission/Deutschland) [Aufsichtsbehörde].

59 Art. 83 Datenschutz-Grundverordnung (Fn. 46).

60 § 43 BDSG-neu (Fn. 48).

61 *Wolff*, in: Schantz/Wolff, Datenschutzrecht, 2017 (Fn. 23), Rn. 1130.

62 EuGH Rs. 39/72, BeckEuRS 1973, 33652 Rn. 17 – Kommission ./. Italien; EuGH Rs. 94/77, BeckEuRS 1978, 67092, Rn. 22/27 – Zerbone.

63 BT-Drs. 18/11325, S. 110 f.; *Wolff*, in: Schantz/Wolff, Datenschutzrecht, 2017 (Fn. 23), Rn. 243.

64 Vgl. Art. 6, Art. 7 Datenschutz-Grundverordnung (Fn. 46). mit Art. 5 und Art. 6 DSRL.

- Das unmittelbar anwendbare Recht versucht mit wenigen Normen die Datenverarbeitung ganz unterschiedlicher Konstellationen zu erfassen, vom Brötchenkauf bis zum Gesundheitscheck und der Steuerverwaltung.
- Das unmittelbar anwendbare Recht enthält eine unendliche Anzahl von Ermächtigungen an die Mitgliedstaaten. Diese sogenannten Öffnungsklauseln knüpfen zudem systematisch an unterschiedliche Ansatzpunkte an und lösen so interne Spannungen aus.[65]

  Das Datenschutzrecht war innerhalb der rechtsetzenden Instanzen in erheblicher Weise umstritten. Das Parlament verfolgte eine stark grundrechtsbezogene Perspektive; die Kommission versuchte erfolglos sich selbst weitreichende Konkretisierungsbefugnisse zuzuweisen; der Rat hatte die nationale Verwaltung und den Verantwortlichen stärker im Blick. Dazu kamen nationale Sonderwünsche. Die geschaffenen Normen besitzen daher Kompromisscharakter.[66]
- Das europäische Recht sieht Mechanismen der Konkretisierung vor. Zu diesem Mechanismus gehören wie gesagt Selbstregulierung der Wirtschaft,[67] die in Deutschland keine Tradition bricht sitzen.
- Weiter gibt es ein starkes Abstimmungsprinzip der Datenschutzbehörde auf europäischer Ebene.[68] Die Summe von jeweils einem Vertreter einer Aufsichtsbehörde aus jedem Mitgliedstaat bildet zusammen einen Europäischen Datenschutzausschuss, der die Auslegung der Datenschutzverordnung zur Aufgabe hat[69] und das unmittelbar anwendbare Recht in Europa für die Aufsichtsbehörden bestimmen soll. Die Beschlüsse wirken aber nur für die Aufsichtsbehörden und nicht für die Gerichte. Müssen die Gerichte Streitigkeiten entscheiden, müssen Sie unmittelbar auf dem europäischen Recht urteilen. Die deutschen Gerichte dürfen dabei das europäische Recht nicht konkretisieren sondern müssen, sofern sie letztinstanzlich entscheiden, den Europäischen Gerichtshof einschalten,[70] was sehr viel Zeit kostet.

Diese Unsicherheit hat zur Folge, dass die Unternehmen und die Bürger oft nicht genau wissen, was das Datenschutzrecht von ihnen verlangt. Es besteht daher eine Unsicherheit, bis das oberste zuständige Gericht, das ist hier der EuGH, die Auslegungsfragen entschieden hat. Bis zu diesem Zeitpunkt werden die Unternehmen versuchen durch Kontaktaufnahmen mit den Aufsichtsbehörden einen für sie gangbaren Weg zu vereinbaren. Das Recht wird daher zwischen Behörde und Unternehmen zum Teil vereinbart. Das ist unglücklich, weil es relativ umständlich ist.

V. Praxisprobleme des Datenschutzes

Die Unbestimmtheit ist nicht das einzige spezifische Problem, das im Datenschutzrecht besteht. Das Datenschutzrecht hat in Europa eine Komplexität erreicht, die ungewöhnlich ist und den Umgang sehr schwierig werden lässt. Dies liegt an verschiedenen Gründen.

1. Unterschiedliche Akteure

Es gibt unterschiedliche Akteure für unterschiedliche Fragen mit unterschiedlichen Kompetenzen. Zunächst ist da der Gesetzgeber. Die Befugnis, Normen für den Datenschutz zu erlassen, ist aufgeteilt auf die Europäische Union einerseits, dem Bundesstaat Deutschland andererseits als auch den Ländern in Deutschland. Es gibt daher drei Regelungsebenen, wobei mitunter zwischen dem Landesgesetzgeber, dem Bundesgesetzgeber und dem europäischen Gesetzgeber Absprachen und Koordination erforderlich sind.

---

65 *Wolff*, in: Schantz/Wolff, Datenschutzrecht, 2017 (Fn. 23), Rn. 218 ff.

66 *Schantz* in: Schantz/Wolff, Datenschutzrecht, 2017 (Fn. 23), Rn. 199.

67 Art. 40-Art. 43 Datenschutz-Grundverordnung (Fn. 46).

68 Art. 60-68 Datenschutz-Grundverordnung (Fn. 46).

69 Art. 64, Art. 65, Art. 70 Datenschutz-Grundverordnung (Fn. 45).

70 S. Art. 267 AEUV s. http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A12012E%2FTXT.

Beim Vollzug der Regelung sind Aufsichtsbehörden zuständig,[71] die von dem der staatlichen Verwaltung vollständig getrennt sind. Sie besitzen auch keine Verbindung zu dem Gesetzgeber oder den Ministerien. Darüber hinaus sieht das unmittelbar anwendbare Recht in Europa vor, dass für einen Verarbeiter, der mehrere Unternehmen und Niederlassungen innerhalb der Europäischen Union besitzt, eine Aufsichtsbehörde zuständig ist und zwar die, welche sich am Sitz der Geschäftsleitung befindet.[72] Die Aufsichtsbehörden sollen dabei miteinander kooperieren.[73] In Deutschland gibt es 18 selbstständige Aufsichtsbehörden, diese müssen sich untereinander verständigen und ein Vertreter von ihnen muss sich dann mit den anderen Aufsichtsbehörden in Europa verständigen.[74]

Von den Aufsichtsbehörden, die selbstständig arbeiten und europäische europaweit miteinander kommunizieren, sind wiederum die Gerichte zu unterscheiden. Die Gerichte besitzen eine erhebliche Rolle, auch bei dem Schutz der betroffenen Personen gegenüber den Aufsichtsbehörden.[75] Die nationalen Gerichte wiederum dürfen aber, da es Union ist, das Recht letztlich nicht allein verbindlich auslegen, sondern benötigen den EuGH. Letztinstanzliche Gerichte haben bei Auslegungszweifeln eine Vorlagepflicht.[76] Diese drei unterschiedlichen Akteure sind nicht wirklich gut miteinander verknüpft, so dass jeder zunächst das machen wird, was er für richtig empfindet, bis der EuGH dann verbindlich Vorgaben erlassen wird.

2. Regionale Hoheitsgewalt bei weltweitem Datenfluss

Die zweite Schwierigkeit besteht darin, dass die Behörden und die staatliche Gewalt regional auf ihr Hoheitsgebiet beschränkt sind, die Daten demgegenüber unbeschränkt über das Internet wandern. Das europäische Recht versucht die Beachtung seiner Regeln auch gegenüber Unternehmen durchzusetzen, die sich an die Verbraucher in Europa wenden, auch wenn sie keine eigene Niederlassung in Europa besitzen.[77] Dies führt dazu, dass die Aufsichtsbehörden gegenüber eine Datenverarbeitung vorgehen muss, die gegebenenfalls im Ausland stattfindet.

3. Hoher Datenschutzstandard

Das dritte Problem ist der hohe Standard des Datenschutzes. Nimmt man den Datenschutz wörtlich, ist er kaum zu erfüllen. Streng genommen müsste jeder Professor, der auf seinem Computer noch ein Gutachten eines PHD-Studenten hat, dieses unmittelbar nach Abschluss des Verfahrens löschen.

4. Wandernde Daten

Das wirkliche Problem des Datenschutzes besteht darin, das Erfordernis der dauernden Rechtfertigung in Wirklichkeit umzusetzen. Daten werden häufig mit Einwilligung erhoben und dann weiterverarbeitet und weitergegeben, mit der Folge, dass eine Person, wenn sie die Verarbeitung nicht mehr will, oft nicht mehr weiß, wo die Daten sind. Das Datenschutzrecht versucht diesem Problem Herr zu werden, indem sie für die betroffene Person Informationsrechte normiert, nachdem diese erfährt, wo die Daten hingehen. Die Wirklichkeit sieht aber etwas anders aus.

VII. Schluss

Das Datenschutzrecht ist in Deutschland im Moment in einer Übergangsphase, die für die Personen, die die Daten verarbeiten, eine große Unsicherheit herbeiführt. Das objektive Recht ist schwer auszulegen und man versucht die Lösung darin zu finden, dass man sich konkret mit der Behörde verstän-

---

71 Art. 51 ff. Datenschutz-Grundverordnung (Fn. 45); §§ 8 ff. BDSG-neu und § 40 BDSG-neu (Fn. 48).

72 Art. 56 i.V.m. Art. 27 Datenschutz-Grundverordnung (Fn. 46).

73 Art. 60 Datenschutz-Grundverordnung (Fn. 45).

74 §§ 17-19 BDSG-neu (Fn. 48).

75 Art. 78 Datenschutz-Grundverordnung (Fn. 45).

76 Art. 267 AEUV (s. Fn.70)

77 Art. 3 Datenschutz-Grundverordnung (Fn. 46).

digt, die zuständig ist. Die Wirtschaft leidet unter diesem Umstand und der Datenschutz kostet erheblich Geld im Augenblick. Es profitieren demgegenüber die betroffenen Personen, da mit ihren Daten nun sehr viel vorsichtiger umgegangen wird, als bisher.

Ich bedanke mich für Ihre Aufmerksamkeit